IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

APPLICANT(s):	Bensimon	CONF. NO.:	3004
SERIAL NO.:	10/719,303	ART UNIT:	2131
FILING DATE:	11/21/2003	EXAMINER:	Zia, Syed
TITLE:	METHOD FOR ESTABLISHING AND MANAGING A TRUST MODEL BETWEEN A CHIP CARD AND A RADIO TERMINAL		
ATTORNEY DOCKET NO.:	886-011604-US (PAR)		

Mail Stop Appeal Brief-Patents
Commissioner of Patents
P.O. Box 1450
Alexandria, VA 22313-1450

PRE-APPEAL BRIEF REQUEST FOR REVIEW

This is in response to the Final Rejection mailed 17 April 2008 and the Advisory Action mailed 10 September 2008 in regard to the above-identified patent application. A Notice of Appeal is being filed concurrently herewith.

The Examiner has made the following errors in the Final Rejection and Advisory Action.

1. In section 2 of the Final Rejection and in the penultimate paragraph on page 3 of the Advisory Action the Examiner states that Julin discloses, "...method for establishing and managing a trust model between an identification module and a radio terminal..." as recited in claim 1.

   It is respectfully submitted that contrary to what the Examiner asserts in the Final Rejection, the relationship between the active card and the retailer terminal in Julin is not <u>a trust relationship</u>. Julin does not disclose a <u>trust model</u> with the <u>radio</u>

terminal as in the claimed invention. Indeed, in Julin's personalization system, the retailer terminal <u>does not need to be trusted</u>. The transmitted personalization data between the SIM card and the central computer *via* the retailer terminal are secured because the data is encrypted by the central computer. This data can only be decrypted by the active card because the Ksim key is only known by the central computer and by the active card as mentioned in lines 10-24 of column 4. The retailer terminal does not participate in the computer and the active card; the retailer terminal is only an element of Julin's system to transmit secured data like the network of this system. The card-identifying information ICC-ID transmitted from the active card to the central computer *via* the retailer terminal are information known by any user of the terminal and does not need to be secured. Thus, the retailer terminal disclosed by Julin is not the claimed <u>trust model</u> and consequently the relationship between the terminal and the active card is not a relationship based on a trust model.

Further, in Julin, a <u>central computer</u> contains means for calculating Ksim on the basis of card information ICC-ID transferred from the retailer place, means for generating IMSI, Ki and PUK, means for encrypting the latter ones using the key Ksim and an A3/A8 algorithm, and means for DES line encryption. This makes <u>the relationship between active card</u> and a <u>central computer</u> secure and trustworthy. In his arguments in the Advisory Action, the Examiner wrongly considers the central computer as being the presently claimed radio terminal. However, in Julin the terminal used by the user is the data terminal 9 linked to an active card reader 12. Thus, the relationship considered as trustworthy by the Examiner is between the central computer and the active card and <u>not</u> between the terminal and the active card. This is true since <u>the terminal is only a means to transfer information</u>, like the network, between the reader of the active card and the central computer. The terminal is member of the trustworthy relationship taught by Julin.

Also, in the system disclosed in Julin, the terminal is an interface between the central computer and the active card as shown in Figure 1 of Julin. On the other hand, in the system of the claimed invention, the SIM card is used as the interface between a secured server (OTA) and the terminal to authenticate and control a trust relationship with the terminal as shown in Figure 1 of the present application. Thus, the organization of Julin differs from the system of the claimed invention because the purpose of the active card with the retailer terminal differs from the purpose of the SIM card with the trust terminal. Consequently, the claimed method is not disclosed in Julin.

Further, it is respectfully submitted that the Examiner is not able to distinctly point out specific lines or referenced elements of the prior art to back up his arguments. He cites almost the whole description without precisely mentioning, for example, which part of the description is used to anticipate that "the retailer terminal is controlled by the active card to authenticate the terminal." He also simply cites the text of the prior art as disclosing that the "retailer terminal can be understood as a trust terminal". It is submitted that this is improper (See 37 CFR 104(c)(2); *Ex Parte Gambogi*, 62 USPQ2d 1209, 1212).

2. Claim 1 also recites, "...controlling by said identification module at least one specific characteristic of the radio terminal, said specific characteristic being previously transmitted by radio-telephony to said identification module from a secured server of said mobile radio-telephony network. It is respectfully submitted that the Examiner is in error when he states that these features are disclosed in Julin.

In particular, the active card of Julin does not carry out a controlling a specific characteristic of the retailer radio terminal to determine whether or not the relationship with this terminal is a trust relationship. Indeed, the retailer terminal is able to get data (ICC-ID) from the active card but does not provide its own data to

permit its identification. The only data provided by the retailer terminal to the active card are the encrypted data transferred from the central computer as mentioned in lines 10 to 20 of column 4.

Further, this step would be useless as the retailer terminal does not need to have a trust relationship with the active card. Moreover, the retailer terminal does not receive a specific characteristic through a <u>secure server</u> as recited in claim 1.

Further, Julin discloses that the card manufacturer and the central computer are informed by the system operator about master key as stated by the Examiner in the Advisory Action. However, <u>there is no characteristic previously transmitted to the terminal and no characteristic of this terminal is controlled to determine a trust relationship between the active card and the terminal</u> as recited in the claim 1.

3. Claim 21 recites, "...a device for memorizing at least one authentication algorithm...a device for memorizing a specific characteristic of the radio terminal..."

It is respectfully submitted that Julin is not arranged to memorize an authentication algorithm or a characteristic of the radio terminal as stated by the Examiner in the Final Rejection. First, the DES algorithm is not an authentication algorithm and no authentication algorithm is disclosed in Julin. Second, lines 63 to 67 of column 3 disclose information ICC-ID preprogrammed in the active card inserted in the pertaining reader during the manufacture of the card. Indeed, at the time of the manufacture of the active card, the reader destined to receive the active card is not known and thus, specific characteristics of the reader cannot be preprogrammed in the active card.

Claim 21 also recites, "...a device for imitating a revocation and a revocation device for revoking said authentication key...a device for activating an updating algorithm for updating said authentication key..."
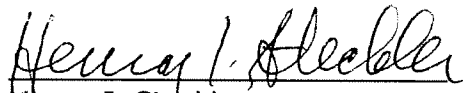
Julin simply discloses the transfer and the loading of personalization information into an active card. The operations and devices mentioned in Julin do not disclose any revocation or updating of the authentication key as presently claimed.

Thus, it is submitted that many essential elements needed for a prima facie rejection under 35 U.S.C. 102(e) are lacking, and the rejection cannot be sustained. Further, since there is no suggestion in Julin of the claimed features, the claims are also unobvious over it (see MPEP 2143.01).

For all of the foregoing reasons, it is respectfully submitted that all of the claims now present in the application are clearly novel and patentable over the prior art of record, and are in proper form for allowance. Accordingly, favorable reconsideration and allowance is respectfully requested. Should any unresolved issues remain, the Examiner is invited to call Applicants' attorney at the telephone number indicated below.

The Commissioner is hereby authorized to charge payment of $990 for the second and third months' extension of time ($120 was charged for the first month on 18 August 2008 with the filing of the After Final Amendment) as well as any other fees associated with this communication or credit any over payment to Deposit Account No. 16-1350.

Respectfully submitted,

Henry I. Steckler   Oct. 13, 2008
Reg. No. 24,139   Date
Perman & Green, LLP
425 Post Road
Fairfield, CT 06824
(203) 259-1800
Customer No.: 2512